Final ePortfolio Submission

Analysis of Cybersecurity Department Organizational Placement

Introduction

As cybersecurity threats increase in frequency, sophistication, and regulatory visibility, organizations must make careful decisions about how to structure and position cybersecurity functions. The placement of a cybersecurity department within a large, publicly traded company has direct implications for governance, operational effectiveness, regulatory compliance, and strategic resilience. This analysis examines the pros and cons of four potential organizational homes for the cybersecurity function: Information Technology (IT), Finance, Operations, and direct reporting to the Chief Executive Officer (CEO).

Option 1: Placement under Information Technology Pros

- **Technical alignment:** Cybersecurity often relies on IT infrastructure, network controls, and system monitoring. Having security embedded within IT ensures direct access to technical staff and resources.
- **Operational efficiency:** Centralized under IT, security teams can integrate controls directly into system design, patching, and maintenance processes.
- **Cost management:** Shared resources (e.g., monitoring tools, infrastructure budgets) may reduce redundancies and promote efficient spending.

Cons

- **Conflict of interest:**

How can IT leaders balance their focus on uptime and efficiency with the stricter requirements of cybersecurity?

IT teams are often measured on uptime, speed of delivery, and

cost savings, which may conflict with security's emphasis on risk reduction and

stricter controls.

- **Limited visibility:** Cybersecurity risks often extend beyond IT, including human resources, physical operations, third-party vendors, and financial systems. Housing cybersecurity under IT may narrow the department's perspective.

•

.

• •

- Does this mean the company could face penalties if cybersecurity is only under IT?"

Option 2: Placement under Finance Pros

- **Risk and compliance alignment:** Finance functions are deeply involved in Sarbanes-Oxley (SOX) compliance, internal controls, and reporting. Cybersecurity threats increasingly pose material financial risks, making Finance a logical home.
- **Investor assurance:** Public companies are under scrutiny to disclose cybersecurity governance. Having cybersecurity report into Finance may enhance perceptions of accountability and fiduciary responsibility.
- **Risk quantification:** Finance teams are skilled at assessing financial impact, which can help translate cybersecurity threats into business terms for executives and investors.

Cons

Board and investor confidence: For a publicly traded company, cybersecurity reporting only through IT may appear insufficiently independent, particularly in light of increasing SEC disclosure expectations

• **Limited technical expertise:** Finance professionals may lack the deep technical background needed to evaluate and prioritize security initiatives effectively. Could Finance leaders overcome this limitation by hiring cybersecurity specialists or relying on consultants?"

• **Slower decision-making:** Financial controls tend to be process-heavy, which may slow response time during security incidents.

• **Operational disconnect:** Finance may not have direct authority over IT systems, operations, or vendors, leading to challenges in implementing timely protections.

Option 3: Placement under Operations Pros

- **Enterprise-wide scope:** Cybersecurity is no longer just a technology issue; it affects supply chains, manufacturing systems, logistics, and customer-facing operations. Embedding security in Operations recognizes this broad scope.
- **Resilience focus:** Operations teams prioritize business continuity, resilience, and disaster recovery—all areas closely linked to cybersecurity.
- **Cross-functional coordination:** An operations-led model may help integrate cybersecurity into day-to-day business processes and risk management.

Cons

- **Dilution of focus:** Operations leaders may prioritize efficiency, productivity, and cost control over stringent security measures.
- **Potential for underinvestment:** Unlike Finance, Operations may lack regulatory drivers to prioritize cybersecurity investments.
- **Technical dependency:** Operations may not have the direct IT expertise required to implement effective cybersecurity strategies.

Option 4: Direct Reporting to the CEO Pros

- **Strategic visibility:** Elevating cybersecurity to a CEO-level report underscores its importance as a core business risk rather than a technical issue.
- **Independence:** A direct line to the CEO reduces conflicts of interest and ensures cybersecurity concerns are not subordinated to IT delivery, financial targets, or operational efficiency.
- **Board-level communication:** This structure facilitates direct reporting to the board of directors, which aligns with SEC guidance and investor expectations for public companies.
- **Cross-enterprise authority:** A CEO reporting line empowers cybersecurity to coordinate across IT, Finance, Operations, HR, and third parties.

Cons

- **Executive bandwidth:**

How can a CEO realistically oversee cybersecurity without being overwhelmed by day-to-day details?

- **Resource allocation:** Without ties to IT, Finance, or Operations, the cybersecurity team may struggle to secure needed resources unless the CEO remains consistently engaged.
- **Implementation challenges:** While visibility improves, execution still depends heavily on IT and Operations, requiring strong partnership structures.

Conclusion and Recommendation

Each placement option carries advantages and trade-offs:

- **IT** provides technical alignment but risks conflicts of interest.
- **Finance** strengthens compliance and investor confidence but lacks operational

and technical depth.

- **Operations** broadens enterprise scope but may dilute focus.
- **Direct to CEO** ensures independence and strategic visibility but relies heavily on

cross-functional cooperation.

For a large publicly traded company subject to regulatory oversight and investor expectations, the most effective structure is often a **hybrid approach**: establish cybersecurity as an independent function reporting to the CEO (or Chief Risk Officer, if present) with strong dotted-line collaboration to IT, Finance, and Operations. This model balances visibility, independence, and execution capability while signaling to regulators and stakeholders that cybersecurity is a top enterprise priority.

cybersecurity may be impractical day-to-day.

CEOs already juggle multiple priorities; direct oversight of

Questions

Does this mean the company could face penalties if cybersecurity is only under IT?”

Could Finance leaders overcome this limitation by hiring cybersecurity specialists or relying on consultants?”

How can IT leaders balance their focus on uptime and efficiency with the stricter requirements of cybersecurity?

How can a CEO realistically oversee cybersecurity without being overwhelmed by day-to-day details?

To: [Head of the organzation]

From: Jabari Thompson
Guarding the Core: Where Cybersecurity Belongs in Our Organization Date: [9/7/2025]
Subject: Recommendation on Placement of Cybersecurity Department

I would recommend the cybersecurity department report to the head of the organization directly to the CEO in order to attain independence, enterprise-wide authority, along with strategic visibility.

Introduction

As we start to build our cybersecurity program, one of the most important choices we have to make is where this department will live in the company. I've looked at the options placing it under IT, Finance, Operations, or reporting directly to you and after considering

the pros and cons of each, my personal conclusion is that it should report directly to you, the CEO. I'd like to give you my reasoning and provide a thorough picture of the options.

1. IT Pros

- IT has technical capabilities and infrastructure, so cybersecurity would have direct access to systems and technical staff.
- Being a part of IT might allow for easy implementation of security controls on time.
- Cost can be reduced by using shared tools and resources. •

Cons

- IT is interested in keeping systems running smoothly and efficiently, and this might sometimes conflict with strict security priorities.
- Cybersecurity risks go beyond IT systems, third-party vendors, human factors, and business processes can be overlooked.
- Investors or the board might view this as less independent. **2. Under Finance Pros**

- Finance possesses risk management and compliance experience, which is relevant to cybersecurity functions.
- Having cybersecurity here can provide investors with more comfort with respect to oversight.
- Finance can translate risks into business terms, which is helpful for decision
- making.

Cons

- Finance does not have deep technical expertise, which can be a problem in evaluating complex security issues.
- Decision-making can be more delayed because of finance processes.
- Finance does not directly control IT systems or operations, which could be a

problem in execution.

3. Under Operations Pros

- Operations have an enterprise-wide view, overseeing supply chains, manufacturing, and other activities affected by cyber threats.
- Focus on business continuity and resiliency aligns well with security goals.
- Integration of security into operations processes may normalize procedures across

the firm.

Cons

- Operations prioritize efficiency and productivity, which may conflict with security demands.
- Without regulatory pressure, cybersecurity may not get its due attention and investment.
- Operations depend on IT for technical implementation, which may slow the process.

Option 4 Reporting Directly to CEO Pros

- Cybersecurity would be completely exposed at the top level, with the clarification that it's an inherent business risk, and not merely technical.
- It keeps cybersecurity independent of IT, Finance, or Operations priorities.
- It enables communication of risks to the board and investors.
- It gives authority to coordinate across the whole company, including IT, Finance,

Operations, HR, and vendors.

Cons

- Oversight would require your time, which could be challenging.
- The department would require positive relationships with IT and other departments

in order to perform effectively.

The teams Recommendation

Having weighed all the alternatives, I firmly think that cybersecurity needs to report to you, the CEO, directly. This structure ensures independence, gives the function visibility at the topmost level, and shows regulators and investors that we're serious about it.

I appreciate the challenges specially making the department work closely with IT, Finance, and Operations but those can be solved with clear dotted-line relationships. That gives cybersecurity both authority and the ability to act.

Conclusion

Cybersecurity is a company-wide issue, not just an IT issue. Placing the department under me signals that the security of our systems, data, and business continuity is a priority. The organization will allow us to respond to threats effectively, meet regulator expectations, as well as investor and board trust.

Sincerely,
Jabari Thompson.

The CIA Triad and the Difference Between Authentication & Authorization

The CIA Triad of Confidentiality, Integrity, and Availability is the foundation for cybersecurity policy and design. With sufficient authentication and authorization controls, these fundamentals ensure that information remains private, is accurate, and is accessible to the correct users at the correct time.

The CIA Triad is the most popular model in cybersecurity. It consists of three terms confidentiality, integrity, and availability.

Confidentiality makes sure the confidential information is only visible to the appropriate parties. This is achieved via numerous methods such as encryption, multi-factor authentication (MFA), access control lists, and user education to prevent phishing and social engineering attacks. (cia)

Integrity ensures that data is reliable and accurate at every stage of its life cycle. Checksumsversioning,digitalsignatures andbackuparetypicallyappliedby organizations to ensure if data has been modified and recover it if it gets corrupted.

Availability ensures that qualified users can access information and systems when needed. Availability is typically provided through redundancy, failover sites, regular patching, and disaster recovery planning to minimize downtime and ensure reliability of systems.

All these three ideas operate as a system as a whole. For example encryption of data assures confidentiality but can hurt availability if decryption keys are lost—demonstrating the purpose behind treating all three of them as a system. (oswap)

Authentication vs. Authorization

Even though the CIA Triad sets the goals of cybersecurity, authentication and authorization are the two most important processes that apply to them.

Authentication is an identity verification process filling out a user or system to verify they are whoever they claim to be. Examples are passwords, biometrics, or MFA codes.

Authorization follows authentication and defines what an authenticated user can perform. Role-based access control and access control lists are common ways of managing authorization.

Authentication asks, Who are you? while authorization asks, What can you do? Both are crucial to secure systems and data.

Examples

In a payroll application, a user is authenticated via a username, password, and MFA code authentication. Upon login the system checks the role of the user. Payroll administrators alone can view payroll records, while regular employees are not allowed even upon successful authentication.

A real-life example is an airport. Presenting your passport to security is authentication but presenting a boarding card at the gate is authorization, confirming permission to board a specific flight.

Conclusion

CIA Triad remains a basis of cybersecurity, which requires organizations to control data confidentiality, accuracy, and availability. Authorization and authentication complement such standards to protect access and authorization. Collectively, they form an effective

measure to defend information systems against threats while ensuring usability and reliability.

Jabari Thompson

Tittle: Using SCADA to Protect Critical Infrastructure and Systems

BLUFF

Critical infrastructure such as water plants energy grids and manufacturing facilities is the foundation on which our society exists. Yet in today's environment, infrastructure is at more risk than ever before from both cyber and physical standpoints. SCADA systems mitigate some of those risks by giving operators an overview and level of control of processes. Simultaneously, SCADA has its own vulnerabilities to be addressed in order for the infrastructure to be truly secure.

Introduction

Electricity water, transportation, and manufacturing systems serving our daily needs are the invisible critical infrastructure on which most people seldom focus. At the heart of so many of these functions are SCADA systems-monitoring and coordinating everything from water treatment pumps to power generation turbines. According to Using SCADA to Protect Critical Infrastructure and Systems from Cyberpal, SCADA setups typically include a combination of hardware and software: HMIs for operators, supervisory server RTUs and PLCs. These components work in concert to gather real-time data, display it to the operators, and ensure that critical processes remain within safe limits. While this connectivity does allow for much more effective control, it also opens the door to a whole new kind of security threat that didn't exist when many of these systems were first designed.

Vulnerabilities in Critical Infrastructure and SCADA

Many SCADA systems were designed and developed a long time ago when cybersecurity was not an issue. They often use outdated or unencrypted protocols such as Modbus or DNP3. As noted in the Cyberpal article, these older systems were originally isolated from the internet, but now that most are connected through modern networks, attackers can exploit those weak points. Other major issues include poor authentication and weak network segmentation. ISA's "9 SCADA System Vulnerabilities and How to Secure Them" notes that many facilities continue to use shared or default passwords, and their control systems are often not segregated from business IT networks, which provides easier pathways for a cyber intruder to move from one system to another. Human error is another major risk. SCADA often relies on operators observing alarms and intervening in automatic controls. Mistakes, misconfigurations, and even phishing attacks targeting employees can have serious consequences. Outdated hardware and unpatched software make things even worse. Because critical infrastructure systems cannot afford to go down for maintenance, updates are often postponed, sometimes leaving known vulnerabilities open for

many years. If an attacker manages to exploit such a weakness, then shutdowns, damaged equipment, or even public safety hazards may occur.

How SCADA Systems Help Mitigate Risks

Even with those challenges, SCADA plays a key role in protecting infrastructure when it's properly managed. Real-time monitoring and alarming: SCADA constantly gathers data from sensors and field devices. If something goes wrong-such as a pump overheating or a pressure drop-the system will immediately notify operators to take quick action.

Data logging and trend analysis: SCADA logs operational data over time. This historical information enables the identification of abnormal patterns, performance tracking, and sometimes predictive maintenance to prevent failures before they occur. System redundancy:

The Cyberpal article notes that many modern SCADA systems have backup servers and multiple communication links to allow for continued operations in case one part of the system fails. Security improvements include the use of secure communication protocols, such as OPC UA and IEC 61850 in addition to industrial VPNs and firewalls. These upgrades protect the data and limit access to trusted users only. In all SCADA not only makes systems more efficient but also provides the visibility and control that operators need to keep critical processes safe and stable.

Conclusion

SCADA systems provide critical infrastructure management, equipping operators with the necessary tools to monitor, control, and protect key services. However, those same systems making operations easier will give way to serious vulnerabilities if not properly secured. The one thing most clear from the article and its cited research is that protection of critical infrastructure isn't merely about installing technologies but responsibly maintaining them, training people on their safe usage, and continuous adaptation to new emerging threats.

Organizations can maintain strong security practices that will keep the systems resilient, and the infrastructure we all depend upon will also continue to function safely and reliably with the new improved SCADA designs